ISSN 1392-0561. INFORMACIJOS MOKSLAI. 2017 79

INFORMACINĖ VISUOMENĖ

Rizika socialiniuose tinkluose: būsimųjų teisėsaugos pareigūnų informuotumas

Edita Butrimė

Mykolo Romerio universiteto
Viešojo saugumo fakulteto docentė, daktarė
Faculty of Public Security,
Mykolas Romeris University, Assoc. Prof., PhD
V. Putvinskio g. 70, LT-44211 Kaunas
El. paštas: edbu@mruni.eu

Vaiva Zuzevičiūtė

Mykolo Romerio universiteto
Viešojo saugumo fakulteto profesorė, daktarė
Faculty of Public Security,
Mykolas Romeris University, Professor, PhD
V. Putvinskio g. 70, LT-44211 Kaunas
El. paštas: vaiva.zuzeviciute@mruni.eu

Pagrindinis tyrimo tikslas buvo atskleisti studentų – būsimųjų teisėsaugos pareigūnų, kurie, kaip tikimasi, ateityje užtikrins kitų žmonių saugumą, informuotumą apie savo ir kitų asmenų saugumą skaitmeninėje erdvėje. Straipsnyje pateikiami teoriniai svarstymai ir empiriniai duomenys (surinkti 2016–2017 m.), kurie padėjo atskleisti, ar būsimi teisėsaugos pareigūnai geba identifikuoti pagrindinius pavojus skaitmeninėje erdvėje ir apsaugoti savo asmeninius duomenis. Tyrimas yra reikšmingas, nes vis daugiau šiuolaikinių socialinio, asmeninio ir profesinio gyvenimo veiklų vyksta skaitmeninėje erdvėje. Jei patys būsimi teisėsaugos pareigūnai negebės atpažinti su skaitmenine sauga susijusių pavojų, jie nebus pakankamai profesionalūs ir pasirengę konsultuoti ir teikti paramą piliečiams minėtais klausimais, kurie yra dominuojantys šiuolaikinio žmogus pasaulyje.

***Reikšminiai žodžiai**: socialiniai tinklai, grėsmės socialiniuose tinkluose, asmens duomenų saugumas.*

Įvadas

Internetas atsirado be plano ir kontrolės, todėl vartotojo saugumo užtikrinimas yra sudėtingas uždavinys (Garšva, Skudutis, 2004). Šiandien, praėjus keliems dešimtmečiams, kartais sunku užtikrinti saugumą internete, nes daugelis priemonių turi būti įdiegtos (ir buvo įdiegtos) vėliau, sprendžiant aktualius saugumo uždavinius internete. Vienas iš sprendimų yra skaidymasis į atskirus segmentus (intranetus) (Vacca, 1997). „Tokie procesai nors ir neišvengiami, prieštarauja visuotinio tinklo idėjai“ (Garšva, Skudutis 2004). Teigiama

(Schneier, 2015), kad technologijos negali išspręsti kompiuterinio saugumo (angl. *computer security*) problemos. Viena iš šios problemos sprendimo sudedamųjų dalių yra technologijos, bet pagrindinė atsakomybė už saugumą tenka žmonėms, kurie technologijas kuria arba jomis naudojasi. XX a. 9-ajame dešimtmetyje atsiradę ir šiandien ypač išpopuliarėję virtualūs socialiniai tinklai iškėlė naujus saugumo virtualioje aplinkoje uždavinius vartotojui. Šiandien virtualiuose socialiniuose tinkluose dalyvauja 2,51 milijardo vartotojų ir prognozuojama, kad 2020 m. jų skaičius pasieks 2,95 milijardo. „Socialinių tinklų masinis paplitimas visuomenėje reiškia, kad kuo daugiau asmenų naudojasi socialinių tinklų paslaugomis, tuo labiau didėja duomenų subjekto teisių pažeidimų tikimybė“ (Malinauskaitė van de Castel, 2017). Daroma išvada, kad asmenys „įgyvendindami savo teises virtualių socialinių tinklų aplinkose <...> gali užtikrinti savo teises tik iš dalies“ (ten pat). Viena iš priežasčių galėtų būti vartotojų žinių apie socialinius tinklus spragos.

Tobulėjant technologijoms ir vis populiarėjant interneto įrankiams, atsiradus galimybei vartotojams kurti turinį internete, duomenų ir vartotojų saugumo problema iškyla kaip kompleksinis uždavinys, kurį turi spręsti IT profesionalai ir vartotojai kartu. Neteisėta veikla, iš pradžių panašėjusi į nekaltus pokštus (1978 m. pirmasis brukalas, kompiuteriniai virusai (pirmasis 1988 m.,) operacinės sistemos veiklai sutrikdyti arba internetinių puslapių išvaizdai pakeisti (angl. *defacement*), ilgainiui tapo vis labiau finansiškai motyvuota, orientuota į tiesioginės piniginės naudos siekimą (Kalpokas, Marcinauskaitė, 2012). Naujausio pokšto pavyzdys: *Microsoft* dirbtinio intelekto *Tay Microsoft* bandymas socialiniame tinkle (Lee, 2016). Bandymas buvo nutrauktas po 24 val., nes dirbtinis intelektas ėmė keiktis ir reikšti rasistines mintis (Vincent, 2016). Šis trumpas įvadas leidžia pagrįsti nuostatą, kad studentai (būsimieji teisėsaugos pareigūnai) turi būti supažindinami su saugumu skaitmeninėje erdvėje, t. y. žinoti, kokių yra grėsmių ir koks elgesys yra saugus.

Pagrindinis tyrimo tikslas – atskleisti, koks yra studentų – būsimų teisėsaugos pareigūnų, kurie, kaip tikimasi, ateityje užtikrins kitų žmonių saugumą, informuotumas apie savo ir kitų asmenų saugumą skaitmeninėje erdvėje.

Uždaviniai:

1. Aptarti sampratas: virtualus socialinis tinklas ir vartotojo duomenų saugumas.
2. Atskleisti virtualių socialinių tinklų vartotojų požiūrį į asmens duomenų saugumą remiantis moksline literatūra.
3. Atskleisti studentų (būsimų teisėsaugos pareigūnų) požiūrį į asmens duomenų saugumą internete (virtualiame socialiniame tinkle).

Tyrimo objektas – studentų veiklos ir asmeninių duomenų saugojimo įpročiai socialiniuose tinkluose. Socialinis tinklas pasirinktas kaip populiariausia studentų laisvalaikio veikla internete.

Straipsnyje pateikiami teoriniai svarstymai ir empiriniai duomenys (surinkti 2016–2017 m.). Išsamiau išdėstytos įžvalgos, kurios jau buvo aptartos ankstesnėje publikacijoje (Butrimė, Zuzevičiūtė, 2016). Šiame straipsnyje pateikiami nauji empiriniai 2017 metų duomenys, tai yra autorės vykdo tęstinį tyrimą, kurio tikslas – nustatyti tendencijas ir modelius.

Socialinis tinklas: keli istorijos momentai ir šiandienos situacija

Virtualus socialinis tinklas (angl. *Online Social Networks* – OSN; *Social Network Sites* – SNS) apibrėžiamas kaip saityno

(angl. *web*) paslauga, leidžianti asmenims: konstruoti viešą ar pusiau viešą paskyrą (angl. *profile*) apribotos sistemos viduje, aiškiai nustatyti sąrašą kitų vartotojų, su kuriais jie turi ryšį, peržiūrėti savo ir kitų vartotojų sukurtų ryšių sąrašą sistemos viduje (Boyd, Ellison, 2007). Asmens duomenys (angl. *personal data*) yra bet kuri informacija, susijusi su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta.

Pirmieji socialiniai tinklai buvo sukurti paskutiniame praėjusio amžiaus dešimtmetyje. Jų vartotojai (Classmates.com pradėjo veiklą 1995 m. lapkričio mėn.) neturėjo galimybės susikurti paskyrų ir draugų sąrašų. SixDegrees.com pradėjo veiklą 1996 m. gegužės mėn. Kiekvienas šio socialinio tinklo vartotojas buvo su kitu susietas ne daugiau kaip per šešis bendrus pažįstamus. Vartotojai turėjo paskyras, galėjo kviesti draugus, organizuoti grupes ir peržiūrėti kitų vartotojų paskyras. Maždaug po dešimties metų Web.2.0 technologijos paskatino reikšmingus socialinių tinklų pokyčius. Šios technologijos yra orientuotos į vartotoją (nesudėtinga vartotojo sąsaja) ir todėl labai patrauklios pradedantiesiems. Technologijų pokytis paskatino netgi tuos žmones, kurie buvo skeptiškai nusiteikę socialinių tinklų atžvilgiu. Kita vertus, toks greitas pokytis (socialinių tinklų vartotojų skaičius sparčiai auga) turėjo pasekmių, nes vartotojai ne visada naudojasi technologijomis saugiai. Net tokioms organizacijoms kaip universitetai sudėtinga saugiai integruoti technologijas ir visą jų potencialą, patrauklų ir naudingą studentams. Web 2.0 įrankiai leidžia spontaniškai, horizontaliai, daugeliu atvejų nekontroliuojamai kurti informaciją ir ja dalintis. Web 2.0 įrankiais naudotis visai paprasta. Tai pritraukia mažiau patyrusius interneto vartotojus. Iš čia kyla nesaugaus dalinimosi skaitmeniniu turiniu grėsmė, nes beveik kiekvienas vartotojas (tas, kuris moka) gali dalintis, gali pasiekti įkeltą skaitmeninį turinį (Anzai, 2009; Davidson, Waddington, 2010; Fraser, Dutta, 2010). Dėl asmeninės neigiamos patirties stokos socialinių tinklų vartotojai elgiasi neatsargiai. Jie neapsaugo asmens duomenų ar savo paskyrų ir, žinoma, įrašų – nuotraukų, filmų, tekstų.

Saugumo skaitmeninėje erdvėje aspektai

EUROSTAT[1] duomenimis, 2015 m. Europos Sąjungoje 1 iš 4 interneto vartotojų susidūrė su saugumo problemomis. S. Jastiuginas (2011) teigia, kad įvertinus informacijos saugumo incidentų mastą, galima teigti, kad individų ir organizacijų netinkamas pasirengimas valdyti informacijos saugumo incidentus gali lemti visos valstybės ir net pasaulines problemas, todėl gebėjimas valdyti informacijos saugumą turi tapti strateginiu tiek organizacijų, tiek valstybių tikslu. Tik valstybės, suvaldžiusios informacijos saugumo problemą savo viduje, gali tinkamai prisidėti prie tarptautinio lygmens rizikos valdymo (CIO, CSO and PwC study, 2010; Ernst & Young's 12th Annual Global Information Security Survey; NATO, 2010). Skandalo, susijusio su „Panama Papers", pavyzdys iliustruoja prieštaravimus, su kuriais susiduria kiekviena organizacija ir valstybė – atskleidžia nevienareikšmį nusikaltimų pobūdį. Nors įsilaužimas yra nusikaltimas, tačiau tos pačios įsilaužimo priemonės internete naudojamos slepiamiems nusikalstamiems duomenims pasiekti. Nutekinti duomenys atskleidė neetišką ir net potencialiai bau-

[1] 2015 m. Europos Sąjungoje vienas iš keturių interneto naudotojų susiduria su saugumo problemomis (EUROSTAT). February 11, 2016.

džiamąjį procesą, kuris, paradoksalu, gali būti laikomas kova su nusikalstama veikla (The International Consortium of Investigative Journalists, 2016). Kai kurie iš šių aspektų jau tapo, o kiti dar taps (tobulėjant technologijoms) dominuojančia būsimųjų teisėsaugos pareigūnų darbo dalimi.

2008 m., kai *Facebook* buvo dar palyginti nauja technologija, buvo atliktas tyrimas, kuriame dalyvavo 1740 JAV studentų (Lewis, Kaufman, Christakis, 2008). 1710 studentų (98,3 % respondentų) buvo *Facebook* vartotojai. K. Lewis, J. Kaufman ir N. Christakis (2008) teigia, kad studentas daug labiau linkęs turėti privačią socialinio tinklo paskyrą, jei: 1) jo draugai (ypač kambario draugai) turi privačias paskyras; 2) jei jis yra aktyvus *Facebook* vartotojas; 3) jei studentas yra moteris; 4) jei jis / ji dalijasi populiariais muzikos įrašais. Autoriai daro išvadą, kad riba tarp privatumo ir viešumo yra peržengta: vartotojai per daug privačių duomenų skelbia viešojoje erdvėje, o dėl to gali būti prarastos darbo galimybės arba – dar blogiau – galimà seksualinė prievarta ar tapatybės vagystė. Autoriai prognozuoja, kad interneto vartotojų, suprantančių privatumo esmę, dėka turėtų atsirasti naujos kartos virtuali erdvė (angl. *self-regulating systems*), kur keičiamasi idėjomis ir socialiniais ryšiais ir kur nesaugi sąveika turėtų būti peržiūrėta. Kartų teorijos tyrinėtojai teigia, jog Z kartos atstovai kitaip suvokia asmens duomenų saugumą socialiniuose tinkluose – jie gali pateikti nepažįstamam asmeniui ne tik savo, bet ir artimų žmonių (tėvų, senelių, brolių, seserų) asmeninius duomenis (Palfrey, Gasser, 2011).

Kai kurie autoriai teigia, kad šiuolaikinių kompiuterių sistemų saugumą užtikrinti yra iš esmės neįmanoma dėl interneto struktūros ir saugumo užtikrinimo standartų. Šiandien internetas techniškai sukuria galimybę šiuolaikiniam pasauliui siekti atvirumo ir žodžio laisvės (Garšva, Skudutis, 2004). Tokią galimybę užtikrina vartotojų anonimiškumas internete. Apibendrinant galima atkreipti dėmesį į susidariusios situacijos dvilypumą: viena vertus, siekiama saugumo užtikrinimo priemonių internete, kita vertus, vartotojų anonimiškumas yra atvirumo ir žodžio laisvės garantas.

Metodologija ir empirinis tyrimas

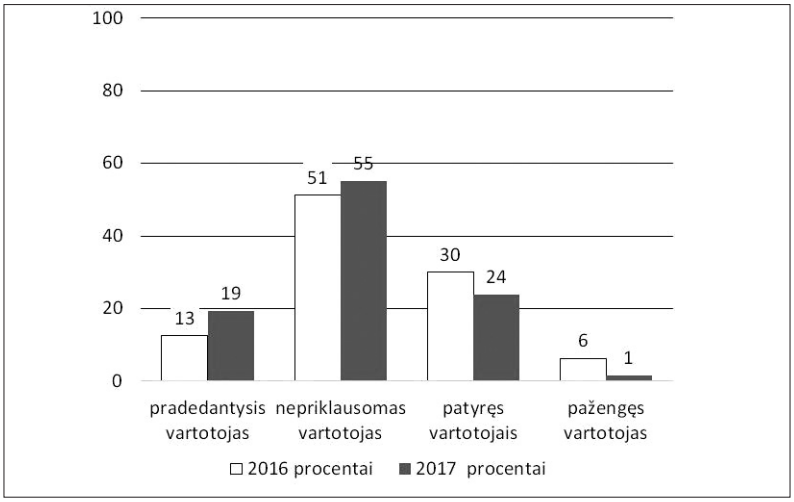
I etapas. N=147 (80 – 2016 m. ir 67 – 2017 m.). Respondentai yra antro ir trečio kurso studentai – būsimieji teisėsaugos pareigūnai. Amžius – nuo 19 iki 23 metų.

Studentai testą atliko semestro pradžioje. Vienas iš klausimų – kaip jūs vertinate savo gebėjimą naudotis paieškos internete įrankiais? (1 pav.). Pusė studentų vertino savo gebėjimus kaip nepriklausomo vartotojo. 2016 m. 30 % respondentų, o 2017 m. 24 % vadino save patyrusiu vartotoju. Galimi pasirinkimai buvo šie: pradedantysis vartotojas, nepriklausomas vartotojas, patyręs vartotojas ir pažengęs vartotojas („aš interneto ekspertas“).

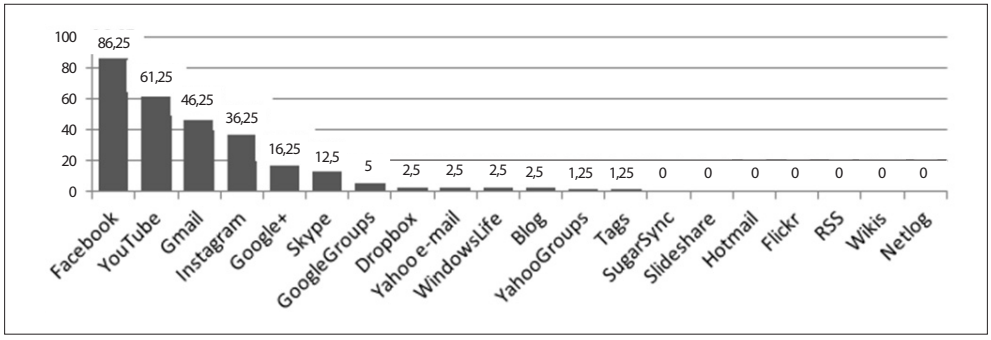
Studentams buvo užduotas klausimas, kokius interneto įrankius jie naudoja savo kasdienėje veikloje (2 pav.). Populiariausias tarp studentų yra socialinis tinklas *Facebook*. Daugelio įrankių studentai nenaudoja visai arba naudoja labai retai. Tarp šių nenaudojamų įrankių – debesų technologijos (*Dropbox*, *SugarSync*) (1 arba 2 studentai iš 80-ies).

II etapas. N=147. Studentų prašyta užpildyti tyrimo instrumentą, kuris parengtas vykdant projektą „Langas į ateitį“ (2015). Testas parengtas atsižvelgiant į Lietuvos Respublikos visuotinio kompiuterinio raštingumo standarto reikalavimus, taip pat į kitų programų (ECDL[2], Microsoft

[2] European Computer Driving Licence (ECDL)



1 pav. ***Studentų atsakymai į klausimą, kaip jūs vertinate savo gebėjimą naudotis paieškos internete įrankiais*** *(procentai)*



2 pav. ***Studentų kasdienėje veikloje naudojami interneto įrankiai*** *(procentai)*

Unlimited Potential Community Learning Curriculum, Microsoft Digital Literacy Curriculum v.2) nustatytus reikalavimus.

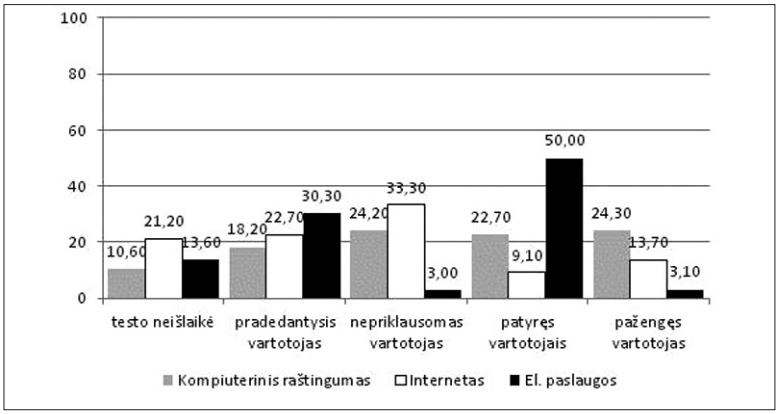
„Langas į ateitį“ (2015) tyrimo instrumento vertinimai: jei respondentas surinko mažiau negu 60 % taškų – testo neišlaikė; 60–70 % – pradedantysis vartotojas; 70–80 % – nepriklausomas vartotojas; 80–90 % – patyręs vartotojais; daugiau kaip 90 % – pažengęs vartotojas (3 pav.).

Šiame tyrimo etape buvo siekiama išsiaiškinti respondentų kompiuterinio raštingumo, gebėjimo naudotis interneto el. paslaugomis lygį. Naudotas standartizuotas testas.

Teste tarp kitų klausimų buvo pateikti tokie, kurie atspindi kompiuterio vartotojo gebėjimą elgtis saugiai:

Klausimų blokas „Kompiuteris“:

- Kuriais atvejais galite būti tikri, kad virusai nepateks į Jūsų kompiuterį?
- Ar antivirusines programas reikia nuolat naujinti, kad atpažintų ir naujai atsiradusius virusus?
- Ką darysite įtarę, kad Jūsų USB atmintukas užkrėstas kompiuterių virusais?



3 pav. ***II etapo standartizuoto testo rezultatai: studentų gebėjimai*** *(procentai)*

Klausimų blokas „Internetas“:

- Kuo skiriasi interneto duomenų perdavimo protokolai, žymimi http ir https?

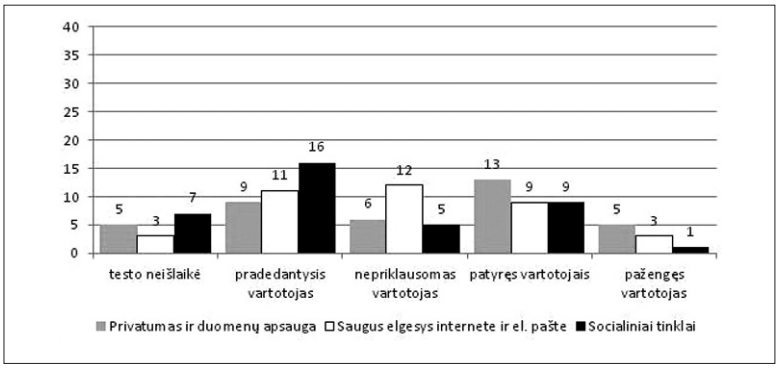
Klausimų blokas „El. paslaugos“:

- Ar saugu pirkti prekes internetu?
- Kas yra elektroninis parašas?
- Ką daryti gavus banko el. laišką su nurodymu pranešti savo internetinės bankininkystės prisijungimo slaptažodį?
- Kas gali nutikti, jei internete atskleisite savo asmens duomenis (pavyzdžiui, vardą, pavardę, gimimo datą ar kredito kortelės numerį)?

III etapas. N=38. Studentai buvo paprašyti atlikti specialų ECDL testą, kuriuo buvo vertinami saugaus elgesio internete gebėjimai. Testą studentai atliko po paskaitos apie duomenų saugumą ir internetinę etiką. Imtis yra patogioji – dalyvavo studentai, kurie tuo metu klausėsi paskaitos. Reikšmingų apibendrinimų nebūtų galima daryti. Apklausos rezultatai bus naudojami tik kaip tam tikrų galimų tendencijų rodikliai ir leis numatyti naujus tyrimus, siekiant gauti patikimesnius duomenis.

Kaip matyti iš 4 pav., studentai stengiasi apsaugoti savo asmens duomenis. Asmens duomenų saugumas apklausos dalyviams yra reikšmingas.

Tie studentai (4 pav.), kuriems saugumas internete atrodė reikšmingas, taip pat buvo



4 pav. ***Studentų žinios apie saugą: privatumas, saugumas internete ir el. pašte, saugumas socialiniuose tinkluose*** *(respondentų dažniai)*

pažengę vartotojai – 9 (ketvirtadalis iš 38). Studentų saugaus elgesio internete ir naudojimosi elektroniniu paštu gebėjimai yra neblogi, nes daugiau kaip pusė studentų (4 pav.) pagal pirmiau išvardytus aspektus buvo identifikuoti kaip nepriklausomi, patyrę ir pažengę vartotojai. Vis dėlto studentų gebėjimai naudotis socialiniais tinklais (kurie yra populiariausias studentų įrankis) yra prastesni. Tyrimų rezultatai parodė, kad beveik pusė studentų (4 pav.) identifikuoti kaip pradedantieji vartotojai. Apibendrinant galima teigti, kad studentai (būsimi teisėsaugos pareigūnai) šiek tiek rūpinasi asmens duomenų apsauga, susirašinėjimo, kito teikiamo turinio skaitmeninėje erdvėje apsauga, privatumu, tačiau menkiau, negu prasminga šiandienos nesaugiame pasaulyje.

IV etapas. N=89. Studentai buvo paprašyti paaiškinti, kaip jie vertina savo saugumą socialiniuose tinkluose. Buvo užduoti du uždarieji klausimai apie *Facebook* (Kiek studentas turi draugų socialiniame tinkle? Kiek socialinio tinklo draugų studentas pažįsta asmeniškai?). Užduoti atvirojo tipo klausimas: 1) Kokie yra socialinių tinkle privalumai ir trūkumai? Parašykite, kaip saugote savo privatumą socialiniuose tinkluose; 2) Ar žinote, kas gauna jūsų į *Facebook* įkeliamą medžiagą?

Analizuojant atsakymus į minėtus klausimus vienas respondentas iškrito iš konteksto. Jis nurodė, kad turi 1188 draugus ir visus juos pažįsta. Respondentas komentavo, kad negali pasakyti, kiek iš savo *Facebook* draugų pažįsta gerai. Šio respondento atsakymas į atvirą klausimą parodė, kad jis domisi bendravimo internete grėsmėmis: „<...> dabar, kai yra plačiai naudojami socialiniai tinklai mūsų visuomenėje, nėra saugu, nes kuo toliau, tuo daugiau atsiranda visokiausių virusų, ir kas svarbiausia, kad kai kurie žmonės niekaip nesuvokia, kad tai virusai. Nors kartais būna taip akivaizdu <...>“. Respondentas negalėjo pasakyti, kas gauna jo į *Facebook* įkeltą informaciją: „<...> su kuo dalinuosi paprasčiausiai kokiu nors straipsniu, daina ar savo mintimis <...> manau daugelis tai mato.“

Uždarojo klausimo apie *Facebook* draugų skaičių analizė parodė, kad didžiausias „draugų“ skaičius yra 1000, o mažiausias – 45. Gerai pažįstamų draugų didžiausias skaičius 800 (vienas studentas teigė, kad asmeniškai pažįsta tiek savo Facebook „draugų“), mažiausias gerai pažįstamų draugų skaičius – 5. Tik pusė studentų (42) galėjo išvardyti priemones, kurios užtikrina *Facebook* paskyros saugumą.

Pirmo atvirojo klausimo duomenų analizės rezultatai leido suskirstyti studentus į tris grupes:

1. Studentai nėra tikri, kad tinkamai ir pakankamai kontroliuoja savo saugumą („Manau, kad nieko aš nekontroliuoju...“).
2. Studentai pripažįsta, kad *Facebook*'e nėra saugūs („Stengiuosi, kad tik minimalus skaičius žmonių matytų, ką publikuoju profilyje, nes nežinau, kam ir kas ir kaip panaudos turinį“; „Nesu tikras, kad informacija apie mane prieinama tik tiems, kuriems tokią teisę suteikiau“; „Nežinau, ar tikrai žmonės yra tie, kas sakosi esą“; „Tiek daug, per daug žmonių žino, ką aš mėgstu, ką darau, kur esu...“; „Savo, kaip vartotojo saugumą skalėje nuo 0 iki 10 įvertinčiau 4“).
3. Studentai teigia kontroliuojantys *Facebook* paskyrą: „Manau, kad tai saugi aplinka, juk aš nusprendžiu, kas yra vieša, kas ne. *Facebook* turi taisykles, jos ir užtikrina vartotojo saugumą <...>“; „Kontroliuoju viską, ką noriu; juk tam yra nustatymai; tik mano draugai mato

viską paskyroje“; „Taip, aš kontroliuoju paskyrą, kam prienami kurie kontaktai, informacija <...>“.

Atsakymus į antrą atvirą klausimą taip pat buvo galima suskirstyti į tris grupes:

1. Studentai jaučiasi nesaugūs socialiniame tinkle. Trys atsakymai: „<...> kiek informacijos apie save dalinsiesi, tiek jos turės ir kiti. Dėl saugumo negalima pasitikėti net žmogum, ką jau kalbėti apie socialinį tinklą“; „Niekur nekeliu jokios medžiagos“; „<...> nesiunčiu nieko asmeniško, jei reikia, pasitelkiu kitas priemones, būdus <...>“.
2. Studentai žino, kad jie negali kontroliuoti turinio, kuriuo dalijasi su socialinio tinklo draugais: „<...> siunčiu vienam asmeniui, o kas gauna vėliau nežinau“; „<...> gauna tas žmogus, kuriam, siunčiu, o kur informacija keliauja vėliau nežinau <...>“.Didžiausia studentų grupė nežino, kaip sklinda turinys socialiniuose tinkluose, nes teigė žinantys, kas gauna jų įkeltą turinį: „<...> kam aš nustatau rodyti ir viešinti savo įkeliamą informaciją, tai tie ir mato, o mano išreikštos nuomonės taip pat yra mano pasirinkimas, kur ir kada ją reikšti <...>“; „<...> taip, kontroliuoju, kas gali matyti mano postus, nuotraukas ir visa kita, kuo aš esu pasidalinusi <...>“.

Išvados

1. Virtualus socialinis tinklas apibrėžiamas kaip saityno paslauga, leidžianti asmenims konstruoti viešą ar pusiau viešą paskyrą apribotos sistemos viduje, aiškiai nustatyti sąrašą kitų vartotojų, su kuriais jie turi ryšį, peržiūrėti savo ir kitų vartotojų sukurtų ryšių sąrašą sistemos viduje. Vartotojo duomenų saugumas – tai visuma priemonių, kurios leidžia apsaugoti asmens duomenis – bet kurią informaciją, susijusią su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta.
2. Empirinis tyrimas parodė, kad du iš trijų universiteto studentų (būsimųjų teisėsaugos pareigūnų) savo gebėjimą saugiai elgtis socialiniuose tinkluose įvardijo kaip „nepriklausomo vartotojo“.
3. Pirmas kokybinio tyrimo klausimas atskleidė tris aspektus: studentai nėra tikri, kad tinkamai ir pakankamai kontroliuoja savo saugumą, pripažįsta, kad *Facebook*’e nėra saugūs, teigia kontroliuojantys *Facebook* paskyrą. Atsakymai į antrą kokybinio tyrimo klausimą leido studentus suskirstyti į tris grupes: tai studentai, kurie 1) jaučiasi nesaugūs socialiniame tinkle; 2) žino, kad negali kontroliuoti turinio, kuriuo dalijasi su socialinio tinklo draugais; 3) nežino, kaip sklinda turinys socialiniuose tinkluose (jie sudaro didžiausią grupę).

Šio keturių etapų tyrimo rezultatai turėtų būti vertinami atsargiai dėl tekste nurodytų apribojimų: patogiosios imties ir mažo dalyvių skaičiaus. Nepaisant to, tam tikros tendencijos ir įžvalgos vis dėlto yra reikšmingos.

Pirma – jauni žmonės, studentai, net būsimi teisėsaugos pareigūnai, aiškiai neatskiria asmeninės ir viešosios erdvių internete. Tai, kad jie neturėjo neigiamos ar net pavojingos patirties, trukdo jiems suprasti prevencijos ir atsargumo būtinumą. Šiandien daug veiklos sričių: studijos, el. bankininkystė, paskolų tvarkymas, el. prekyba ir pan., yra skaitmenizuotos, todėl mūsų kaip švietėjų pareiga nuolat jauniems žmonėms priminti apie būtinumą būti atsargiems. Net būsimi teisėsaugos pareigūnai yra naivūs ir nepasirengę nei rūpintis savimi, nei konsultuoti kitus.

Antra – faktas, kad jaunieji mūsų kolegos yra gana kompetentingi skaitmeninės erdvės vartotojai (bent jau jų pačių subjektyvia nuomone, kaip parodė mūsų tyrimas), dar nereiškia, kad jie atsargiai ir rūpestingai elgiasi su savo asmeniniais duomenimis internete.

LITERATŪRA

2015 m. Europos Sąjungoje 1 iš 4 interneto naudotojų susiduria su saugumo problemomis (EUROSTAT). February 11, 2016 [interaktyvus] [žiūrėta 2016 m. balandžio 20 d.]. Prieiga per internetą: <http://ivpk.lrv.lt/lt/naujienos/europos-sajungoje-1-is-4-interneto-naudotoju-susiduria-su-saugumo-problemomis>.

ANZAI, Yayoi (2009). Digital Trends among Japanese University Students: Podcasting and Wikis as Tools for Learning. *International Journal on E-Learning*, vol. 8(4), p. 453–467. Chesapeake, VA: AACE.

BOYD, Danah M.; ELLISON Nicole B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, vol. 13, iss. 1, p. 210–230 [interaktyvus] [žiūrėta 2017 m. gegužės 20 d.]. Prieiga per internetą: <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full>.

BUTRIMĖ, Edita; ZUZEVIČIŪTĖ, Vaiva (2016). Students' / future law-enforcement officers' perspective on safety in the digital space. In *Kultura bezpieczeństwa : Nauka – Praktyka – Refleksje*. – Kraków: Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron". ISSN: 2299-4033.

DAVIDSON, Ann-Louise; WADDINGTON, D. (2010). E-Learning in the university: When will it really happen? *eLearning Papers*, No 21, September 2010. ISSN 1887-1542. [interaktyvus] [žiūrėta 2010 m. rugsėjo 30 d.]. Prieiga per internetą: <http://www.elearningeuropa.info/files/media/media23710.pdf >.

FRASER, Matthew; DUTTA, Soumitra (2010). *Mano virtualieji aš. Kaip socialiniai tinklai keičia gyvenimą, darbą ir pasaulį*. Vilnius: Eugrimas. 476 p. ISBN 978-9955-790-78-5

GARŠVA, Eimantas; SKUDUTIS, Julius (2004). Secure Computer System design. *Electronics and Electrical Engineering*, vol. 6(55), p. 43–48.

JASTIUGINAS, Saulius (2011). Information Security Management in Lithuania's Public Sector. *Informacijos mokslai*, t. 57, p. 7–25 [interaktyvus], [žiūrėta 2016 m. balandžio 10 d.] Prieiga per internetą: <http://www.journals.vu.lt/informacijos-mokslai/article/view/3137/2755>.

KALPOKAS, Vaidas; MARCINAUSKAITĖ, Renata (2012). Identity Theft in Cyberspace: Technological Aspects and Criminal Legal Assessment. *Teisės problemos*, Nr. 3(77), p. 30–52.

Langas į ateitį („Window to the Future"). Last modified 2015 [interaktyvus] [žiūrėta 2016 m. vasario 2 d.]. Prieiga per internetą: <http://www.epilietis.eu/index.php/about-the-project>.

LEE, Peter. Learning from Tay's introduction. *Official Microsoft Blog* [interaktyvus] [žiūrėta 2016 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/#sm.000jh14di129ee0ov1u1atn7zsco3>.

LEWIS, Kevin; KAUFMAN, Jason; CHRISTAKIS, Nicolas (2008). Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication*, No. 14, p. 79–126 [interaktyvus] [žiūrėta 2016 m. vasario 2 d.]. Prieiga per internetą: <doi: 10.1111/j.1083-6101.2008.01432.x>.

MALINAUSKAITĖ-VAN DE CASTEL, Inga (2017). *Duomenų subjekto teisės virtualiuose socialiniuose tinkluose*: Daktaro disertacija. Socialiniai mokslai. Vilnius, Mykolo Romerio universitetas. 186 p. [interaktyvus] [žiūrėta 2017 m. gegužės 20 d.]. Prieiga per internetą: <https://repository.mruni.eu/pdfpreview/bitstream/handle/007/14648/Inga%20MalinauskaiteTeiseWWW.pdf?sequence=1 >.

Microsoft's disastrous Tay experiment shows the hidden dangers of AI [interaktyvus] [žiūrėta 2016 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://qz.com/653084/microsofts-disastrous-tay-experiment-shows-the-hidden-dangers-of-ai/>.

PALFREY, John; GASSER, Urs (2008). *Born Digital Understanding the First Generation of Digital Natives*. Published by Basic Books. New York, p. 384 [interaktyvus] [žiūrėta 2017 m. gegužės 20 d.]. Prieiga per internetą: <http://pages.uoregon.edu/koopman/courses_readings/phil123-net/identity/palfrey-gasser_born-digital.pdf>.

SCHNEIER, Bruce (2015). *Secrets and Lies – Digital Security in a Networked World*. John Wiley & Sons. 488 p. ISBN 978-0-471-45380-2.

The International Consortium of Investigative Journalists. *The Panama Papers*. Publication Date: 04/11/2016. Politicians, Criminals and the Rogue Industry that Hides Their Cash [interaktyvus] [žiūrėta 2016 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://community.globaleditorsnetwork.org/content/panama-papers-politicians-criminals-and-rogue-industry-hides-their-cash-0>.

VACCA, John, R. (1997). *Intranet security*. Charles river media Inc. Massachusetts. 458 p.

VINCENT, James (2016). *Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day*. March 24, 2016 [interaktyvus] [žiūrėta 2016 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist>.

RISKS IN SOCIAL NETWORKS: AWARENESS OF FUTURE LAW-ENFORCEMENT OFFICERS

Edita Butrimė, Vaida Zuzevičiūtė

S u m m a r y

The main purpose of this article is to investigate the awareness of students, future law enforcement officers – who will be expected to protect other citizens – on the risks of their personal safety in the digital space. The paper presents both theoretical considerations and empiric data from a study (completed in 2016 and in 2017), dedicated to investigating whether future law enforcement students recognize the main risks for safety in digital space. This study is important in light of the fact that a large part of our contemporary social, personal and professional lives is being carried out in digital spaces. If future law enforcement officers are unable to recognize the risks on safety, they, as a consequence, will not be professional and ready enough to consult and provide support for citizens on the issues that begin, in some cases, to dominate the functioning of a contemporary person in a contemporary world.

Keywords: social network sites, risks in social networks, safety of personal data.

2017 m. birželio 1 d.